1. A method of creating a signed content hash, comprising:

dividing content into a plurality of chunks of content;

hashing each chunk of the plurality of chunks of content into a hash table; and

signing the hash table.

2. The method of claim 1, wherein hashing each chunk of the plurality of chunks of content into the hash table comprises:

calculating a chunk hash of each chunk of the plurality of chunks of content to provide a plurality of chunk hashes corresponding to the plurality of chunks of content; and

storing the plurality of chunk hashes in the hash table.

3. The method of claim 1, wherein dividing the content into the plurality of chunks of content and hashing each chunk of the plurality of chunks of content into the hash table is repeated a plurality of times to create a corresponding plurality of hash tables.

4. The method of claim 1, wherein signing the hash table comprises:

creating a certificate of authenticity of the hash table; and

signing the certificate of authenticity of the hash table.

5. The method of claim 4, wherein the certificate of authenticity of the hash table comprises the hash table in its entirety.

6. The method of claim 4, wherein the certificate of authenticity of the hash table comprises an overall hash of the hash table.

7. The method of claim 6, wherein creating the overall hash of the hash table comprises:

hashing the plurality of chunk hashes stored in the hash table to create the overall hash of the hash table.

8. The method of claim 4, wherein the certificate of authenticity of the hash table comprises additional information relating to the content and a set of rules governing the use of the content.

9. A method of authenticating a content hash, comprising:

authenticating a hash table containing a plurality of chunk hashes corresponding to a plurality of chunks of content;

dividing the content into a plurality of chunks of content; and

authenticating each chunk of the plurality of chunks of content.

10. The method of claim 9, wherein authenticating the hash table comprises:

verifying a certificate of authenticity of the hash table; and

if the certificate of authenticity of the hash table is verified, authenticating the hash table.

11. The method of claim 10, wherein verifying the certificate of authenticity of the hash table comprises:

verifying a signature of the certificate of authenticity comprising the hash table in its entirety; and

if the signature of the certificate of authenticity containing the hash table in its entirety is verified, verifying the authenticity of the hash table.

12. The method of claim 10, wherein verifying the certificate of authenticity of the hash table comprises:

verifying a signature of the certificate of authenticity comprising an overall hash of the hash table;

calculating a recalculated overall hash of the hash table; and

if the recalculated overall hash of the hash table matches the overall hash of the hash table, verifying the authenticity of the hash table.

13. The method of claim 12, wherein calculating the recalculated overall hash of the hash table comprises:

hashing the plurality of chunk hashes stored in the hash table to create the recalculated overall hash of the hash table.

14. The method of claim 10, wherein verifying the certificate of authenticity of the hash table further comprises:

verifying additional information in the certificate of authenticity of the hash table relating to the content and a set of rules governing the use of the content.

15. The method of claim 9, wherein authenticating each chunk of the plurality of chunks of content comprises:

calculating a recalculated chunk hash of the chunk of content to provide a recalculated chunk hash corresponding to the chunk of content;

comparing the recalculated chunk hash to the chunk hash of the chunk stored in the hash table; and

if the recalculated chunk hash matches the chunk hash of the chunk stored in the hash table, verifying the authenticity of the chunk.

16. The method of claim 15, further comprising:

processing the chunk of content by having the recalculated chunk hash of the chunk of content calculated concurrently with calculating the recalculated chunk hash of the chunk.

17. The method of claim 16, wherein processing the chunk of content further comprises:

decrypting the chunk of content; and

rendering the chunk of content to the user.

18. The method of claim 9, wherein dividing the content into the plurality of chunks of content and authenticating each chunk of the plurality of chunks of content is repeated a plurality of times to authenticate a corresponding plurality of hash tables.

19. A method of authenticating digital content, comprising:

calculating an overall hash of a hash table containing a plurality of chunk hashes corresponding to a plurality of chunks of content;

comparing the overall hash of the hash table to a hash contained in a certificate; and

if the overall hash of the hash table matches the hash of the certificate, verifying the authenticity of the plurality of chunks of the content.

20. The method of claim 19, wherein verifying the authenticity of the plurality of chunks if the overall hash of the hash table matches the hash of the certificate, further comprises for each chunk of the plurality of chunks of content:

calculating a hash of the chunk to create a chunk hash of the chunk;

comparing the chunk hash to a stored chunk hash of the chunk stored in the hash table; and

if the chunk hash matches the stored chunk hash, verifying the authenticity of the chunk.

21. The method of claim 20, wherein contemporaneously with calculating the hash of the chunk to create the chunk hash of the chunk, further comprising:

decrypting the chunk to provide a chunk of decrypted content of the content package; and

rendering the chunk of decrypted content of the content package.

22. A method of authenticating digital content, comprising:

dividing content of a content package into a plurality of chunks of content;

calculating a chunk hash of each chunk of the plurality of chunks of content to provide a plurality of chunk hashes stored in a hash table corresponding to the plurality of chunks of content;

hashing the plurality of chunk hashes of the hash table to create an overall hash of the content of the content package;

placing the overall hash into a certificate;

determining whether a recalculated overall hash of the hash table matches the overall hash of the hash table;

if the recalculated hash of the hash table matches the overall hash of the hash table, verifying the authenticity of each chunk of the plurality of chunks of the content.

23. The method of claim 22, wherein determining whether the recalculated overall hash of the hash table matches the overall hash of the hash table comprises:

recalculating the overall hash of the hash table to create the recalculated overall hash;

comparing the recalculated overall hash to the overall hash; and

if the recalculated overall hash matches the overall hash and a signature on the certificate is valid, verifying authenticity of the hash table.

24. The method of claim 22, wherein verifying the authenticity of each chunk of the plurality of chunks comprises for each chunk:

recalculating a hash of the chunk to create a recalculated chunk hash of the chunk;

comparing the recalculated chunk hash to the chunk hash of the chunk; and

if the recalculated chunk hash matches the chunk hash of the chunk, verifying the authenticity of the chunk.

25. The method of claim 24, wherein contemporaneously with recalculating the hash of the chunk to create the recalculated chunk hash of the chunk, further comprising:

decrypting the chunk to provide a chunk of decrypted content of the content package; and

rendering the chunk of decrypted content of the content package.